Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	GN Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF T-MOBILE USA, INC.

Cathleen A. Massey
Indra Sehdev Chalk

T-MOBILE USA, INC.
601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004
(202) 654-5900

July 24, 2019

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	GN Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF T-MOBILE USA, INC.

T-Mobile USA, Inc. ("T-Mobile")[1/] submits these comments in response to the *Third Further Notice of Proposed Rulemaking* ("Third FNPRM") in the above-referenced proceedings aimed at protecting consumers against illegal and unwanted robocalls.[2/] We wholeheartedly agree with the Commission that wireless providers play a crucial role in providing consumers tools to battle unwanted and illegal robocalls, and we are proud of the cutting-edge solutions T-Mobile makes available to its customers today for free. We also agree that by working together with the FCC and other industry participants, we can do more to eliminate the scourge of unwanted and illegal robocalls.

I. INTRODUCTION AND SUMMARY

In its Declaratory Ruling, the Commission took an important step in combatting unwanted and illegal robocalls by clarifying that its rules do not prevent carriers from blocking unwanted robocalls.[3/] This clarification resolves an important legal question that will have positive, lasting ramifications on carriers' abilities to deploy new tools and techniques to combat

---

1/ T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.

2/ *Advanced Methods to Target and Eliminate Unlawful Robocalls, et al.*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, CG Docket No. 17-59 & WC Docket No. 17-97 (rel. June 7, 2019) ("*Declaratory Ruling*" and "*Third FNPRM*" respectively).

3/ *Declaratory Ruling* at ¶¶ 22-25, 31.

robocalls. As a companion to this action, the Third FNPRM proposes to establish a carrier safe harbor from liability for call blocking, an important precursor to carriers' establishment of an opt-out call-blocking regime. T-Mobile agrees that a clear and sufficiently broad safe harbor, backstopped by reasonable safeguards to ensure that critical public safety calls are not blocked, will best encourage the widespread deployment of default call blocking.

As the first wireless provider to implement STIR/SHAKEN standards on its network in November 2018, T-Mobile supports industry-wide deployment of STIR/SHAKEN which, when fully implemented, should reduce incidences of illegal spoofing and allow fraudsters to be more readily identified. But the safe harbor should be broader than the current proposal, which would protect voice service providers that offer call-blocking programs that take into account whether a call has been properly authenticated under the STIR/SHAKEN framework and may potentially be spoofed. T-Mobile proposes a more robust, carrier-based safe harbor based on reasonable analytics, *including* STIR/SHAKEN, to block calls. Particularly during the potentially initial uneven implementation of STIR/SHAKEN by all providers, expanding the safe harbor will better protect consumers from unwanted calls and encourage providers to adopt default call-blocking. Without a broad safe harbor like T-Mobile proposes, providers both large and small likely will be hesitant to block calls by default due to concerns about liability stemming from their common carrier obligation to complete calls.

In addition to advocating for a broad safe harbor, T-Mobile:

- agrees that providers should not block critical calls. The Commission should work with industry stakeholders to determine what constitutes a "critical call" and how such a list should be developed and maintained;

- suggests that providers be required to demonstrate STIR/SHAKEN compliance by showing the ability to implement the protocols with at least one large provider;
- opposes the imposition of a uniform display for call authentication; and
- recommends against Commission-based information mechanisms for determining the effectiveness of robocall solutions.

II. T-MOBILE IS THE LEADER IN CALL AUTHENTICATION

T-Mobile has done more than any other carrier to fight unwanted and illegal robocalls. Our state-of-the-art anti-robocalling measures have identified over 15 billion scam calls and blocked over 3.5 billion calls to date.[4/] T-Mobile is proud to have been the first wireless provider to implement STIR/SHAKEN standards on its network in November 2018, and the first to implement cross-network STIR/SHAKEN with Comcast Xfinity.[5/] We were the first to implement STIR/SHAKEN standards on our network with our "Caller Verified" technology on over ten devices with more to come in 2019.[6/] For customers with these devices, the words "Caller Verified" will appear when an incoming call is authentic so the customer knows that the phone number has not been hijacked by scammers.

We have been and will continue to be an active participant in key industry groups aimed at improving caller authentication and combatting unwanted robocalls, such as the ATIS STI-GA

4/ Press Release, T-Mobile, Over 3.5 Billion Blocked … And Counting: T-Mobile Hosts Scam 'Block Party' to Raise Awareness (July 11, 2019), https://www.t-mobile.com/news/scamblockparty.

5/ *See* Letter from Kathleen O'Brien Ham, Senior Vice President, Government Affairs, T-Mobile to Geoffrey Starks, Commissioner, FCC (July 10, 2019) at 2 ("Starks Letter").

6/ *See* Starks Letter at 2.

Board,[7/] the USTelecom Industry Traceback Group,[8/] and the Commission's Robocalling Strike Force.[9/]

As the Un-carrier, T-Mobile continues to find innovative solutions to help customers fight fraud and avoid illegal and unwanted robocalls, and to offer these solutions free of charge.[10/] T-Mobile is the only carrier giving customers *free* scam, spoof, and spam protection at the network level, and virtually our entire subscriber base is protected by these scam-identifying solutions. More than two years ago, T-Mobile introduced Scam ID and Scam Block, network-based tools available to all postpaid T-Mobile customers and Metro by T-Mobile customers. Other carriers require their customers to download applications, use certain devices, change device settings, or opt-in to scam-identifying services—but not so for T-Mobile. With Scam ID, our customers are automatically alerted when an incoming call is likely to be malicious or spoofed by the words "Scam Likely" on their handsets. Customers who do not want to be bothered by any scam calls, can turn on Scam Block by simply dialing #662# from their

---

7/ Marcella Wolfe, *Secure Telephone Identity Governance Authority Launched in Major Industry Effort to Combat Unwanted Robocalling*, ATIS (Sept. 18, 2018), https://sites.atis.org/insights/secure-telephoneidentity-governance-authority-launched-in-major-industry-effort-to-combat-unwanted-robocalling/. The Secure Telephone Identity Governance Authority Board is managed by the industry under the auspices of ATIS and held its first Board meeting in August 2018.

8/ *See* Chloe Sanchez, *Taking Charge Against Robocalls*, USTELECOM (Sept. 26, 2018), https://www.ustelecom.org/blog/taking-charge-against-robocalls. USTelecom has led the 24-member Industry Traceback Group since 2016 to identifying the source of illegal robocalls and working with law enforcement to bring them to justice.

9/ *Statement of Chairman Wheeler on Progress Toward Offering Consumer Robocall Blocking Choices*, FCC (July 25, 2016), https://docs.fcc.gov/public/attachments/DOC-340458A1.pdf. In addition to T-Mobile, the other 15 Members of the Robocall Strike Force were AT&T, Apple, Bandwidth.com, Birch, Blackberry, British Telecom, CenturyLink, Charter, Cincinnati Bell, Comcast, Cox, Ericsson, FairPoint, Frontier, GENBAND, Google, Inteliquent, Level 3, LG, Microsoft, Nokia, Qualcomm, Rogers, Samsung, SilverStar, Sirius/XM, Sprint, Syniverse, US Cellular, Verizon, West, and Windstream.

10/ *See* Starks Letter.

handsets. These call-labeling and blocking solutions have alerted customers to an average of 225 million Scam Likely calls *per week.*[11/]

For customers who want more information about their calls, we offer Name ID for free in all Magenta Plus and T-Mobile ONE Plus plans and for $4 per line per month for other T-Mobile customers. Name ID is pre-loaded on every new Android device (and expected to be available for download on iOS devices in the coming months) so that customers can try it out for 30 days for free and then decide whether to sign-up. Name ID allows customers to directly manage entire categories of robocalls; they can choose whether they want to send "Telemarketing calls," "Political calls," "Nuisance calls," "Survey calls," "Charity calls," "Informational calls," or "Prison/Jail calls" straight to voicemail. It also allows them to manage personal phone number block lists at the network level so that blocked numbers stay blocked even when customers switch to a new device. Name ID also includes reverse number lookup.

We also provide a tool – through this web page – for customers to notify us when calls are inadvertently blocked that are not spoofed. And we work with callers, encouraging them to use services like those offered by First Orion, to ensure that calls are not inadvertently labeled as "Scam Likely."[12/]

III. A BROAD, FLEXIBLE SAFE HARBOR IS IN THE PUBLIC INTEREST

T-Mobile strongly supports the Commission's proposal to provide a safe harbor for providers that implement the STIR/SHAKEN framework. As a carrier that has implemented STIR/SHAKEN, T-Mobile welcomes the certainty of the proposed safe harbor and agrees that it

---

11/ Press Release, T-Mobile, T-Mobile's Network Protects Customers from Over 10 Billion Scam Calls, Expands STIR/SHAKEN Protection (Mar. 6, 2019), https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2019/T-Mobiles-Network-Protects-Customers-from-Over-10-Billion-Scam-Calls-Expands-STIRSHAKEN-Protection/default.aspx.

12/ CALL TRANSPARENCY, https://calltransparency.com/ (last visited Jul 23, 2019).

will help promote more aggressive call blocking. To be truly effective, however, the Commission should make two changes to its proposal. First, it should clarify that the safe harbor will be applied on a *provider basis*. The Third FNPRM does not explicitly state that all calls made by compliant providers will be covered by the proposed safe harbor. Doing so will incentivize providers to offer call blocking on an opt-out basis, further protecting consumers, by ensuring that providers will be covered by the safe harbor even when, despite using reasonable analytics including STIR/SHAKEN, legitimate calls are inadvertently blocked.

Second, the Commission should broaden the safe harbor by covering providers that implement reasonable analytics to block robocalls – *including implementation of STIR/SHAKEN*. Carriers, including T-Mobile, currently use reasonable analytics to identify and block robocalls and those reasonable analytics are being constantly updated. As explained more fully below, providing a safe harbor only for identifying and blocking calls relying on the STIR/SHAKEN framework may unnecessarily limit the widespread deployment of default call blocking to the detriment of consumers.

A. Implementation of STIR/SHAKEN

Using STIR/SHAKEN as a meaningful component for a safe harbor is appropriate and will encourage all providers to adopt the STIR/SHAKEN framework. The greater number of carriers that use STIR/SHAKEN, the more effective it will be – resulting in fewer robocalls, which benefits all consumers.[13/]

The Commission asks if there are other instances under the STIR/SHAKEN framework – besides those in which the attestation header has been maliciously altered or inserted – where

13/ *See Third FNPRM* at ¶¶ 49-58.

authentication would fail, that should lead to call blocking.[14/] As noted above, many robocalls will originate outside of the STIR/SHAKEN framework. But even within that framework, the safe harbor should extend to cover instances where attestation fails for reasons other than malicious alteration or insertion of the attestation header – such as when, as the Commission suggests, an originating provider neglects to update its signing certificate. Blocking under these circumstances will encourage all providers to ensure accurate implementation of the STIR/SHAKEN framework and promote default call blocking. It is unreasonable to oblige a terminating provider to decide *why* a call fails STIR/SHAKEN; failure to meet STIR/SHAKEN should be a sufficient reason to justify call blocking and to qualify for the call-blocking safe harbor.

Providers' ability to rely on the safe harbor by implementing the STIR/SHAKEN framework should not be undermined by carrier decisions to *decline* to block certain types of calls that fail the STIR/SHAKEN authentication framework. Instead, providers should have the option of blocking a failing call or passing it along with as much call information as is available. Consumers may not want all calls that fail STIR/SHAKEN authentication to be blocked. For example, providers may develop the capability, in conjunction with callers, to identify numbers that are spoofed for a valid reason. As the Commission has noted, there are legitimate, legal uses for spoofing – when a doctor calls a patient from her personal mobile phone and displays the office number rather than the personal phone number or a business displays its toll-free call-back number.[15/] And as noted below, consumer-identified calls that fail authentication can be white-listed.

[14/] *See id.* at ¶ 52.

[15/] *See Declaratory Ruling* at ¶ 38 (Noting that "industry has been active in developing solutions that allow callers to communicate with voice service providers and analytics companies to identify themselves

B. Safe Harbor Protections Should Extend Beyond STIR/SHAKEN

To be effective, the safe harbor should not be limited to providers blocking calls under only the STIR/SHAKEN framework; it should also protect providers blocking calls based on the use of reasonable analytics. In its Declaratory Ruling, the Commission confirmed that providers may use reasonable analytics to block calls on an opt-out basis.[16/] If carriers rely on reasonable analytics to block calls on an opt-out basis, the safe harbor should continue to apply.

The Commission reasonably wishes to promote solutions that will result in blocked calls from "bad actors."[17/] STIR/SHAKEN protocols cannot be used to identify "bad actors;" they can only be used to determine if a call originates from a spoofed number. The use of reasonable analytics can go beyond STIR/SHAKEN to identify suspicious calls that it cannot. Moreover, limiting the safe harbor to only those calls failing the STIR/SHAKEN framework would not allow carriers to block the vast majority of robocalls originating outside of the United States. Furthermore, as the Commission notes, not all providers will be able to implement STIR/SHAKEN immediately – if at all.[18/] To encourage these providers to block illegal and unwanted robocalls, on an opt-out basis, the Commission should extend the safe harbor to include blocking based on reasonable analytics. This is important because, however advanced the analytics used by carriers to block calls, there will always be some risk that legitimate calls are inadvertently blocked. Absent a safe harbor to manage this risk, carriers will be more likely

---

and share their call patterns that might otherwise seem to indicate illegal call activity."); *see also* Caller ID Spoofing, FCC, https://www.fcc.gov/consumers/guides/spoofing-and-caller-id (last visited July 23, 2019).

16/ *See Declaratory Ruling* at ¶¶ 34-35.

17/ *See Third FNPRM* at ¶ 55.

18/ *See id.* at ¶¶ 56-57, 78.

to offer call blocking on an opt-in basis only, or else employ more conservative criteria in deciding which calls to block, resulting in more robocalls reaching consumers' devices.

Finally, the Commission seeks comment on ways to protect callers from erroneous blocking.[19/] As noted above, T-Mobile already provides tools to consumers and works with callers to address these so-called "false positives." Just as providers should be free to rely on reasonable analytics to block calls to take advantage of a Commission safe harbor, they should be permitted to establish reasonable procedures to address wanted calls that may otherwise be blocked. The marketplace is in the best position to determine if providers are excessively blocking wanted calls, and the response to that blocking.

IV. PROTECTIONS FOR CRITICAL CALLS

The Commission asks whether it should require any voice service provider that offers call-blocking to maintain a "Critical Calls List" of numbers it may not block.[20/] Carriers, including T-Mobile, are already highly incentivized to make sure that all wanted and legitimate calls are not subject to blocking, including *bona fide* emergency calls. But the question of what constitutes "critical calls" and how they are identified is one that should be decided by the Commission with input from all industry stakeholders, including voice providers and the public safety community. In the meanwhile, T-Mobile continues to develop its network-based tools to ensure that wanted and legitimate calls are not inadvertently blocked.

The Commission seeks comment on the numbers that should be included on a Critical Calls List.[21/] Again, T-Mobile urges the Commission to work with key stakeholders to arrive at

---

19/ *See id.* at ¶ 70.

20/ *See id.* at ¶¶ 63-70.

21/ *See id.* at ¶ 65.

the appropriate definition. For example, calls from PSAPs may be an appropriate starting point since they represent a known and verifiable category of entities for which no blocking may be reasonably implemented. Expanding the category of critical calls beyond PSAPs will present definitional challenges that will make not blocking problematic, unwieldy, and subjective. Carriers like T-Mobile engage in regular outreach to PSAPs, which affords an opportunity to identify and white list those callers, but establishing a white list for other categories of caller would likely present significant practical challenges. Moreover today, at least in T-Mobile's case, consumers can white list other, non-911, calls using our Name ID application. This solution can accommodate a customer's decision to always receive calls from a particular list of callers that present a profile that may trigger blocking, including schools, alarm companies, and other institutions.

The Commission asks about the potential establishment of a centralized "white list" of critical caller numbers.[22/] A centralized list of truly critical callers is appealing on its face but presents many complex issues that must be resolved before implementation, including how to maintain its confidentiality and ensure that numbers on the list are not spoofed. In the meanwhile, voice providers should be covered by the Commission's safe harbor if they use reasonable processes to ensure the completion of emergency calls.

V. MANDATING CALLER ID AUTHENTICATION

As noted above, T-Mobile has already implemented STIR/SHAKEN caller ID authentication, and is therefore prepared to comply with the Commission's proposed deadline.[23/] The Commission asks how providers should be required to demonstrate compliance with

---

22/ *See id.* at ¶ 64.

23/ *See id.* at ¶¶ 71-74; *see also* Starks Letter; Letter from Kathleen O'Brien Ham, Senior Vice President, Government Affairs, T-Mobile to Jessica Rosenworcel, Commissioner, FCC (Jan. 14, 2019).

STIR/SHAKEN implementation.[24/] As the Commission notes, there are two components of STIR/SHAKEN – authentication, or "signing" by the originating provider, and verification (of the signature) by the terminating provider. Providers should be required to certify that they can provide both functions. However, just being prepared to use STIR/SHAKEN is not sufficient – implementation requires testing with cooperating providers. Therefore, in order to demonstrate compliance with STIR/SHAKEN, providers should be required to demonstrate that they have completed implementation protocols with at least one large provider (however the Commission defines that).[25/]

The Commission asks if it should adopt a uniform display showing consumers whether a call has been authenticated.[26/] Providers should be able to offer their own form of display and consumers will ultimately determine whether the display is understandable.[27/] Additionally, it is not necessary for the Commission to have a role in STIR/SHAKEN governance. As it notes, iconectiv has been designated as the policy administrator for STIR/SHAKEN.[28/] It has successfully driven STIR/SHAKEN to this point. Policy and other governance should continue to be industry-based, with the Commission intervening only if and when industry response becomes inadequate.

24/ *See Third FNPRM* at ¶¶ 76-77.

25/ Today, T-Mobile has already implemented STIR/SHAKEN with Comcast Xfinity.

26/ *See Third FNPRM* at ¶ 77.

27/ However, the Commission should require some type of positive display so that consumers can determine in real-time calls that are authenticated.

28/ Press Release, ATIS, Mitigating Illegal Robocalling Advances with Secure Telephone Identity Governance Authority Board's Selection of iconectiv as Policy Administrator (May 30, 2019), https://sites.atis.org/insights/mitigating-illegal-robocalling-advances-with-secure-telephone-identity-governanceauthority-boards-selection-of-iconectiv-as-policy-administrator/; *see also Third FNPRM* at ¶ 71.

VI. MEASURING EFFECTIVENESS OF ROBOCALL SOLUTIONS

The Commission asks whether it should create a mechanism to provide information to consumers about the effectiveness of various voice service providers' robocall solutions.[29/] The Commission need not create that mechanism. Doing so will only result in unnecessary and potentially burdensome data collection requirements. T-Mobile regularly shares such information with consumers through its press releases and social media channels.[30/] Voice service providers that offer a robust set of robocall blocking tools to consumers already have every market incentive to communicate this to customers and potential customers. If voice providers' solutions are ineffective – consumers know and complain.

Assuming the Commission adopts its proposal to mandate STIR/SHAKEN, all providers will employ the framework, making it an industry standard. And by extending the safe harbor to the use of other reasonable analytics, providers will be able to customize their call blocking services. The marketplace will determine the effectiveness of those additional provider solutions.

29/ *See Third FNPRM* at ¶ 83.

30/ *See, e.g.*, Press Release, T-Mobile, T-Mobile's Network Protects Customers from Over 10 Billion Scam Calls, Expands STIR/SHAKEN Protection (Mar. 6, 2019), https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2019/T-Mobiles-Network-Protects-Customers-from-Over-10-Billion-Scam-Calls-Expands-STIRSHAKEN-Protection/default.aspx; Press Release, T-Mobile, T-Mobile Has Blocked Over a Billion Scam Calls, and Now Industry-Leading Tech Keeps Customers Even Safer (Nov. 8, 2018), https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2018/T-Mobile-Has-Blocked-Over-a-Billion-Scam-Calls-and-Now-Industry-Leading-Tech-Keeps-Customers-Even-Safer/default.aspx; *see also* @JohnLegere, Twitter (June 25, 2019, 7:15 AM), https://twitter.com/JohnLegere/status/1143523094499250178 ("PLUS, @TMobile customers can stop robocalls when they opt-in to FREE Scam Block. They'll never even see the "Scam Likely" alerts. Just turn it on in your MyTmobile account or the T-Mobile Name ID app, or dial #662# from your T-Mobile phone #StopBadRobocalls") (emojis omitted).

VII. CONCLUSIONS

The Commission should adopt a broad and clear safe harbor from liability for providers that implement reasonable call blocking analytics, including the use of the STIR/SHAKEN authentication framework. Such a safe harbor will help encourage voice service providers to make call blocking available to consumers on an opt-out basis, improving the market penetration and effectiveness of these tools. By clarifying the scope of the safe harbor, the Commission can significantly increase the availability of default call-blocking tools, while ensuring that critical calls are not adversely impacted. Additionally, the Commission should work with industry and other stakeholders to define and develop a Critical Calls List, starting with PSAPs. If the Commission chooses to mandate STIR/SHAKEN implementation, it should require providers to perform both signing and verification functions, and to demonstrate that they have completed implementation protocols with at least one large provider, but the Commission should not mandate a uniform display showing consumers whether a call has been authenticated. Finally, the Commission should not create a mechanism or mandate additional data collection to measure the effectiveness of robocall solutions.

Respectfully submitted,

/s/ *Cathleen A. Massey*

Cathleen A. Massey
Indra Sehdev Chalk

T-MOBILE USA, INC.
601 Pennsylvania Ave., NW
North Building, Suite 800
Washington, DC 20004
(202) 654-5900

July 24, 2019